IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A method for protecting a host located within a computer network, the method comprising:
mapping a public host address for a public host to a secret host address for a secret host containing data accessible over the computer network, said public host address being available from a domain name system server;
receiving a request for communication with the secret host at the public host;
forwarding said request from the public host to the secret host; and
processing said request at the secret host and communicating from the secret host over the network, wherein said communication appears to be sent from the public host;
wherein forwarding said request comprises:
determining whether an attack is consuming significant resources,
if it is determined that an attack is not consuming significant resources, slowing down the forwarding of said request short of stopping the same, and
if it is determined that an attack is consuming significant resources, stopping the forwarding of said request.

2. (Original) The method of claim 1 wherein the network is the Internet and the secret host is a server.

3. (Original) The method of claim 2 wherein the server hosts a Web site.

4. (Original) The method of claim 1 wherein receiving a request comprises receiving a URL at the domain name system server, the domain name system server providing an IP address of the public host corresponding to the URL.

5. – 6. (Cancelled)

7. (Currently Amended) The method of claim 61 further comprising notifying the secret host of the attack.

8. (Original) The method of claim 7 further comprising tracking down a source of the attack.

9. (Original) The method of claim 8 wherein tracking down a source of the attack comprises performing a trace back at the secret host.

10. (Original) The method of claim 1 further comprising directing one or more clients to send requests to an alternate public host.

11. (Original) The method of claim 10 wherein a notification that the public host is under attack is received at the secret host.

12. (Original) The method of claim 10 wherein a notification that the public host is congested is received at the secret host.

13. (Original) The method of claim 10 wherein the secret host has received a request for heightened security.

14. (Original) The method of claim 10 further comprising requesting the DNS server to replace the public host address with an alternate public host address.

15. (Currently Amended) A computer program product for protecting a host located within a computer network, comprising:
computer code that maps a public host address for a public host to a secret host address for a secret host containing data accessible over the computer network, said public host address being available from a domain name system server;
computer code that receives a request for communication with the secret host at the public host;
computer code that forwards said request from the public host to the secret host;

computer code that processes said request at the secret host and communicates from the secret host over the network, wherein said communication appears to be sent from the public host; and

a computer-readable storage medium for storing the codes;

wherein forwarding said request comprises:

determining whether an attack is consuming significant resources,

if it is determined that an attack is not consuming significant resources, slowing down the forwarding of said request short of stopping the same, and

if it is determined that an attack is consuming significant resources, stopping the forwarding of said request.

16. (Original) The computer program product of claim 15 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave.

17. (Original) The computer program product of claim 15 further comprising code that receives at the secret host a notification that the public host is under attack.

18. (Original) The computer program product of claim 17 further comprising code that directs one or more clients to send requests to an alternate public host upon receiving said notification.

19. (Original) The computer program product of claim 17 further comprising code that requests the DNS server to replace the public host address with an alternate public host address upon receiving said notification.

20. (Currently Amended) A system for protecting a host located within a computer network, the system comprising:

a public host having a public host address available from a DNS server; and

a secret host having a secret host address and containing data accessible over the computer network, said public host address being mapped to said secret host address;

wherein the public host is operable to forward requests received from the network to the secret host and the secret host is operable to process said requests and communicate from the secret host to the network with said communication appearing to be sent from the public host;

wherein forwarding said requests comprises:

determining whether an attack is consuming significant resources,

if it is determined that an attack is not consuming significant resources, slowing down the forwarding of said requests short of stopping the same, and

if it is determined that an attack is consuming significant resources, stopping the forwarding of said requests.

21. (Original) The system of claim 20 wherein the secret host is configured to manage the public host.

22. (Currently Amended) A method for hiding an IP address of a computer node located within a computer network, the method comprising:

associating an IP address for a public node with an IP address of a secret node such that only the public node has access to the IP address of the secret node, said IP address for the public node being available from a DNS server;

receiving packets from the network at the public node;

forwarding said packets from the public node to the secret node; and

responding to said packets at the secret node such that a response appears to be sent from the public node rather than the secret node;

wherein the method further comprises:

determining whether an attack is consuming significant resources;

if it is determined that an attack is not consuming significant resources, slowing down the forwarding of said packets short of stopping the same;

if it is determined that an attack is consuming significant resources, stopping the forwarding of said packets.

23. (Original) The method of claim 22 wherein the packets contain requests for data and the secret node is a server hosting a Web site.

24. (Original) The method of claim 22 wherein the packets contain e-mail.

25. (Cancelled)

26. (Currently Amended) The method of claim ~~25~~2 further comprising requesting the DNS server to replace the IP address of the public node with an IP address of an alternate public node.

27. (Currently Amended) The method of claim ~~25~~2 further comprising directing specific client computers to send packets directed at the public node to an alternate public node.

28. (Original) The method of claim 22 further comprising switching to an alternate public host when congestion at the public host exceeds a predetermined level.

29. (Original) The method of claim 22 further comprising switching to an alternate public host to provide increased security at the secret host.

30. (New) The method of claim 22 wherein, after stopping the forwarding of said packets, said secret node requests that the DNS server replace a current public node IP address with an IP address of an alternate public node, and attempts to track down a source of the attack, where, after the attack has stopped, an IP address of an alternate Post Office Box Internet Protocol (POBIP) node is replaced with an original public node IP address.

31. (New) The method of claim 22 wherein, after stopping the forwarding of said packets, said secret node notifies select clients of an alternate public node IP address, and attempts to track down a source of the attack, where, after the attack has stopped, an IP address of an alternate Post Office Box Internet Protocol (POBIP) node is replaced with the IP address of the public node.